

**Welcome!**



**THE  
CRYPTO  
CURIOUS  
COURSE**

The graphic features a blue-to-red gradient background with diagonal lines. The text 'THE CRYPTO CURIOUS COURSE' is rendered in a bold, yellow, 3D font with a red shadow, slanted upwards from left to right.

# Course Goals

- Learn how to store cryptocurrency securely
- Examine the mechanics behind a cryptocurrency transaction
- Know where to look when something goes wrong
- Explain how cryptocurrency is different than cash
- Understand how blockchain technology may impact YOU!

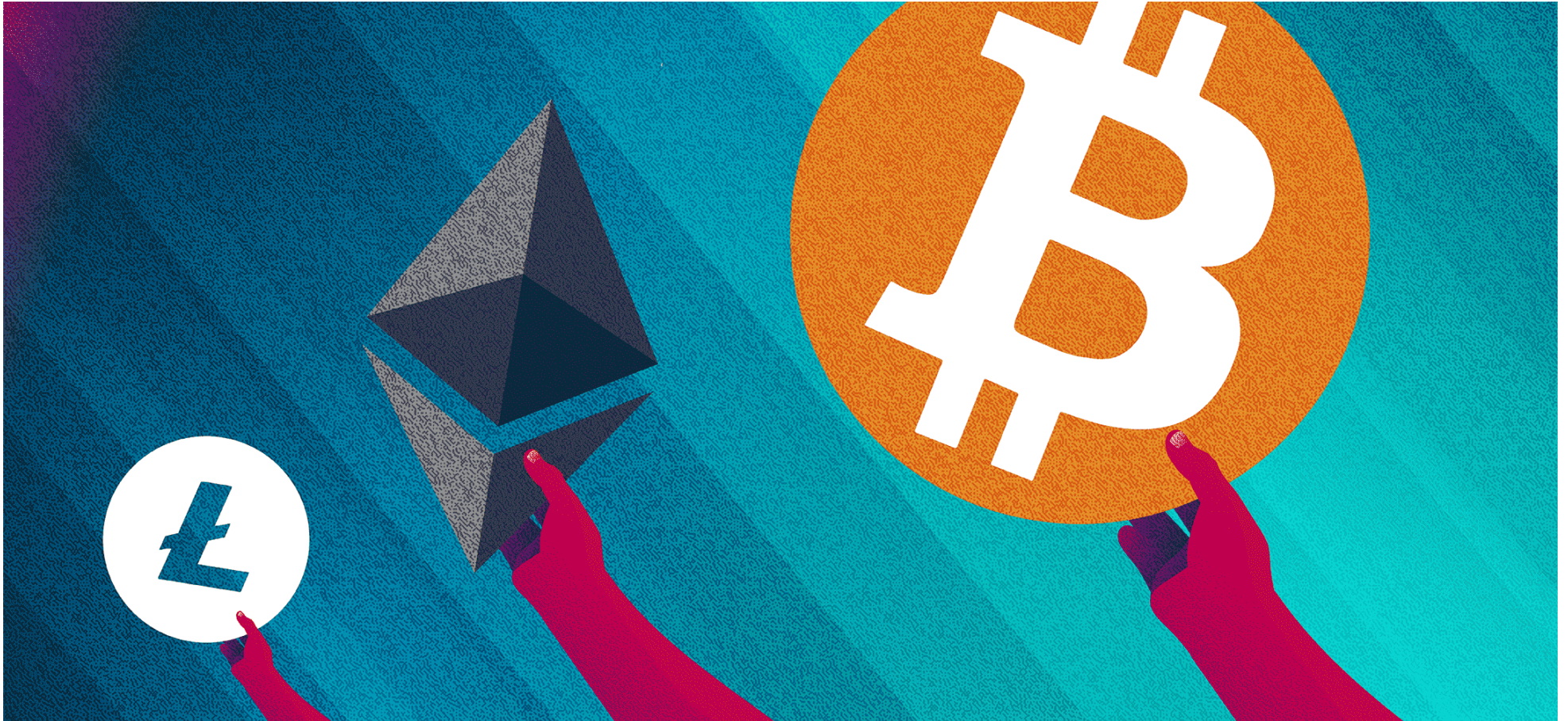




# WHY BITCOIN



# Financial Freedom



[weteachblockchain.org](http://weteachblockchain.org)

*Bitcoin can't be bailed out.*



# Satoshi Nakamoto



[weteachblockchain.org](http://weteachblockchain.org)



# 2008-2009 Global Financial Crisis



**THE TIMES**  
Sat 3 Jan 2009  
Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

## Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

### Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes. *News, page 2*

### Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

**99p**  
Pulp chain cuts the price of a pint from £1.69 to 199p levels. *Business, page 47*

**Michael Sheen, Frost, Nixon and me**  
*Magazine*

**Working mums**  
So that's how she does it  
*Body&Soul*

**Detox in style**  
The best spas on the planet  
*Travel*

**Salman Rushdie**  
I won't marry again  
*Pages 72, 73*

**Giant killing?**  
Guide to the FA Cup third round  
*Sport*

weteachblockchain.org

Front Page of *(The Times)*.





# **THE PROBLEM BITCOIN SOLVES**



# Investment Bank Collapse



[weteachblockchain.org](http://weteachblockchain.org)

Breaking News from [CNN](http://CNN).



# Subprime Mortgage Crisis



[weteachblockchain.org](http://weteachblockchain.org)

Front Page of [\(The Wall Street Journal\)](#), and [\(Daily News\)](#).



# Banks Declared "Too Big to Fail"



[weteachblockchain.org](http://weteachblockchain.org)

*Shannon Stapleton / Reuters via [The Atlantic](#)*



# Digital Uniqueness without Banks

- Blockchain are ledgers that track transactions in a decentralized way
  - Anyone can make a database that maintains uniqueness
  - Digital uniqueness is easy for one computer to enforce
  - Maintaining transactional state across a network is much harder
- Transactions can represent the transmission of money, goods, or data
  - Retail purchase
  - Credentials
- All transactions are time stamped, ordered, and cannot be altered (immutable)
  - Avoids repeat entries
  - Creates a digital fingerprint

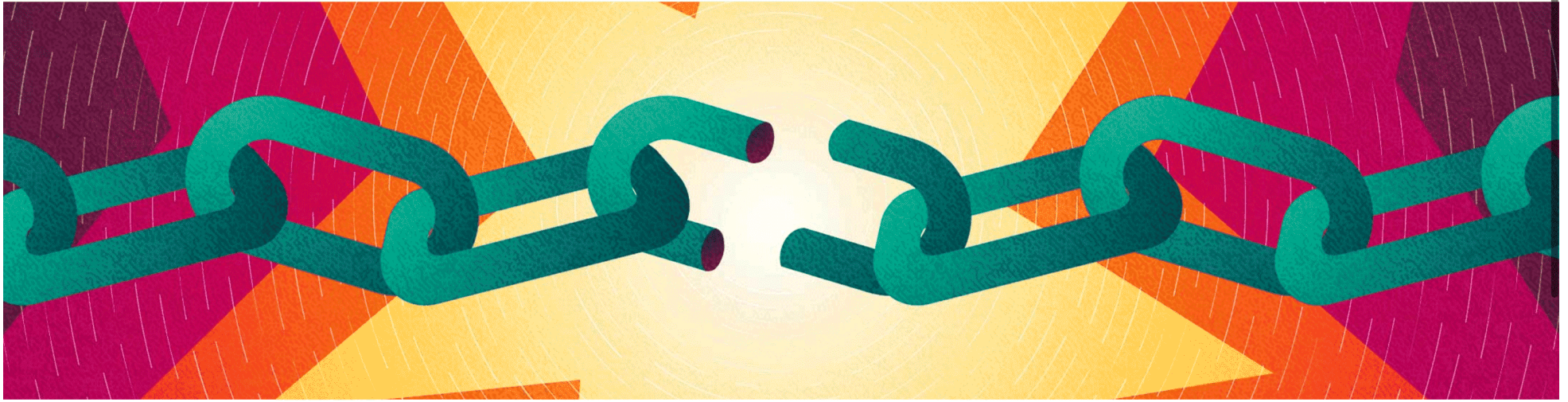




# **THE HISTORY OF CRYPTOCURRENCY**



# The Web and Digital Currency

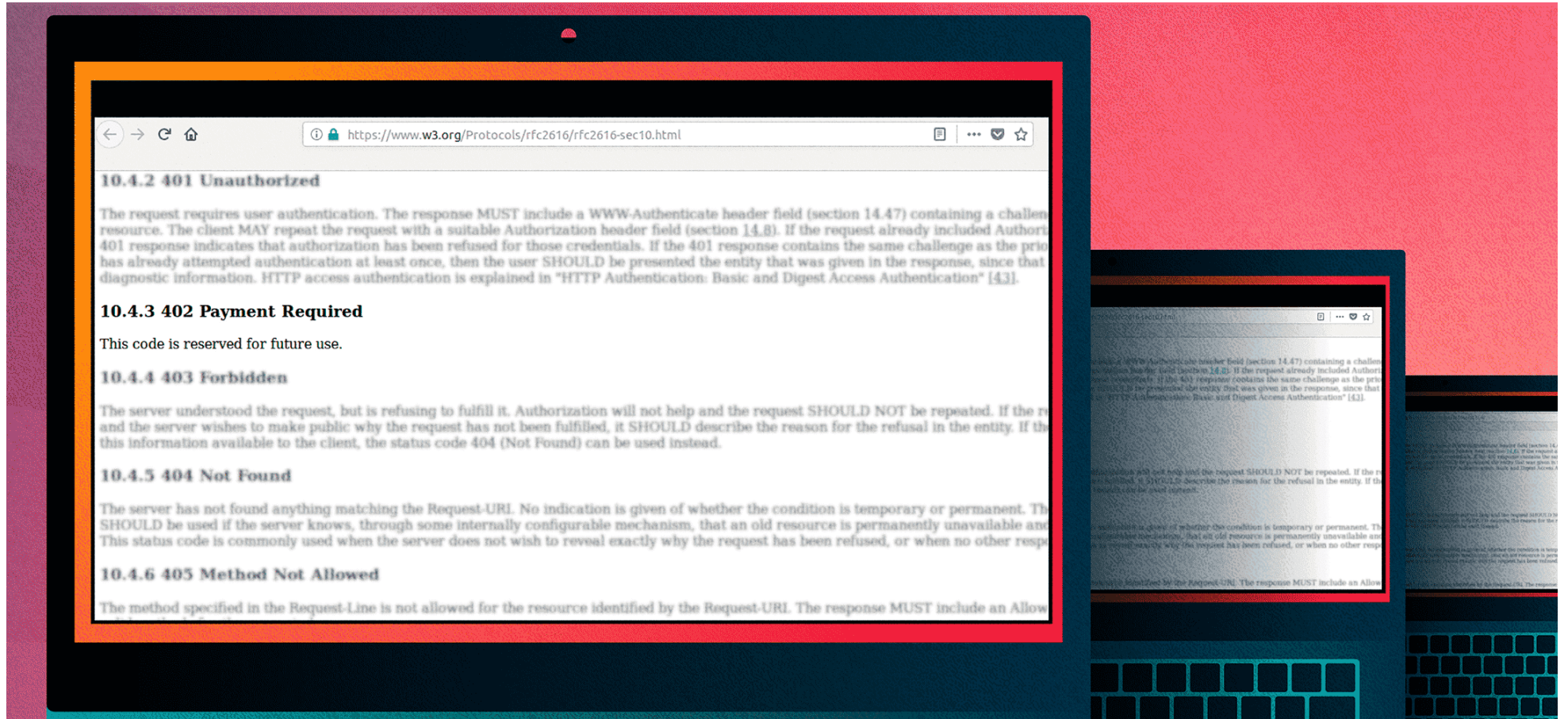


 **Oops! That page can't be found.**

It looks like nothing was found at this location. Maybe try a search?



# Cash for the Internet





# Digital Currency Experiments

**HashCash**

*DigiCash™*

**e-gold**

**Goldmoney®**

 **Liberty  
Reserve**

**B-Money**

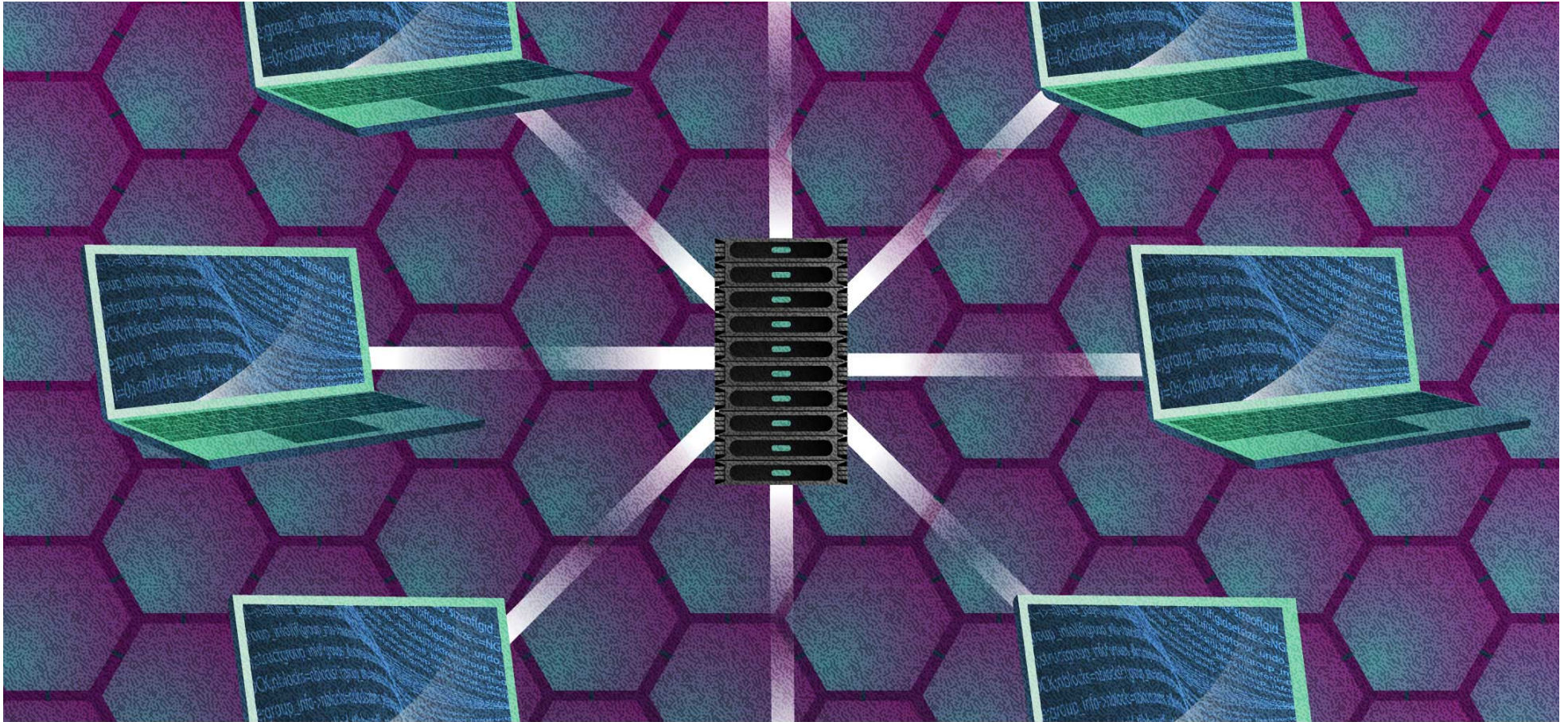


# 1998: PayPal Launched





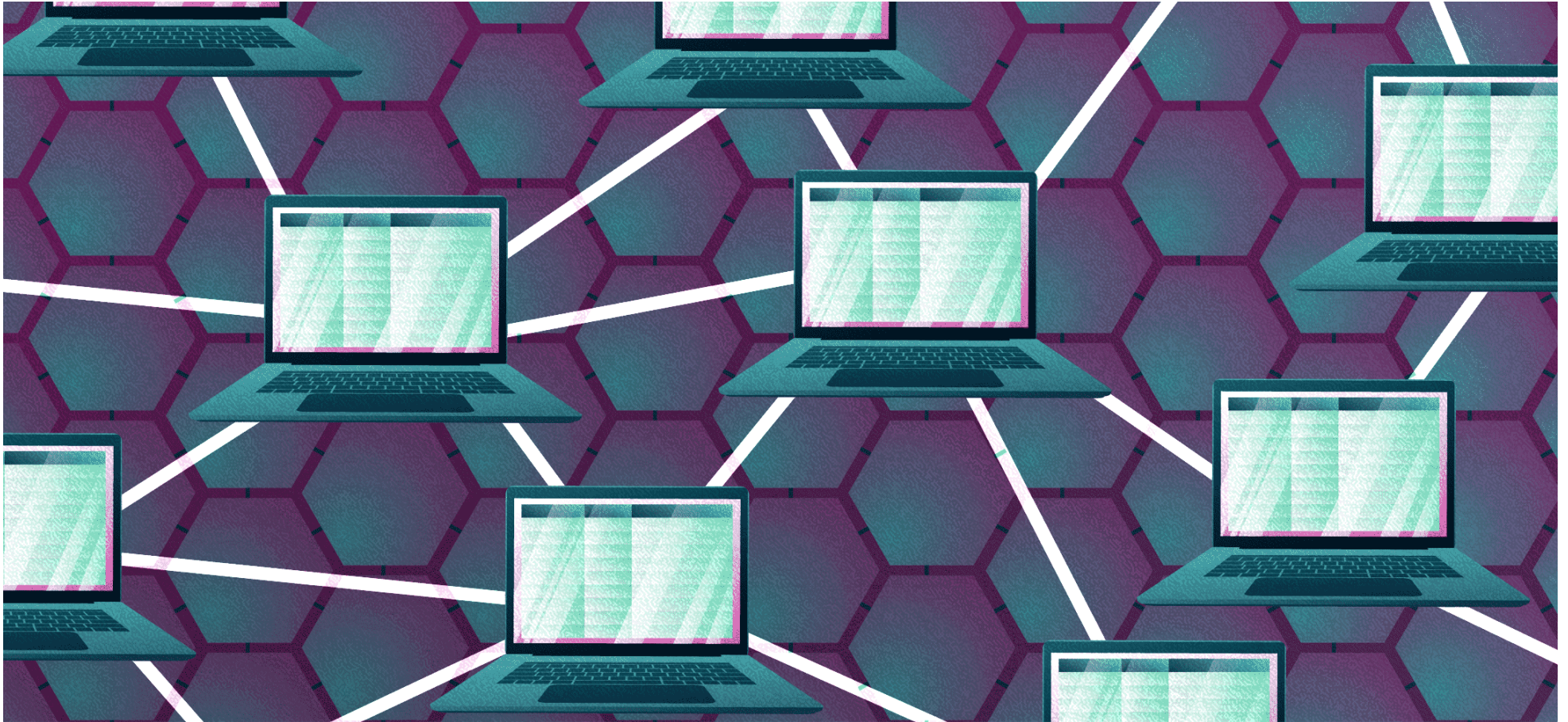
# The Central Server



[weteachblockchain.org](http://weteachblockchain.org)



# The Decentralized Network



[weteachblockchain.org](http://weteachblockchain.org)



# Defining Bitcoin

- Cryptocurrency
  - Digital currency that is created and secured through a “mining process” that uses cryptograph. “Small b” bitcoin is the unit of account for the Bitcoin network
- Blockchain
  - Technological backbone that allows cryptocurrencies to function. The “Big B” Bitcoin network is an example of blockchain technology in action
- “b”itcoin vs “B”itcoin
  - “b”itcoin, the cryptocurrency token changes ownership on the “B”itcoin network—which uses blockchain technology



# The Values Behind Blockchain

- Anti-censorship
  - Resilient to infrastructure problems, intentional or accidental
  - Transactions cannot easily be stopped from reaching the network
- Transparency
  - Triple-entry accounting means proving a cryptographic receipt
  - Malicious server administrator can't make changes
- Trusting Trustless Transactions
  - Transactions can be made even in the absence of trust
  - You want trust, but can't always be with each other in person
  - Internet transactions lack trust that you are used to when dealing in person, instead relying on consumer protection laws to mitigate risk

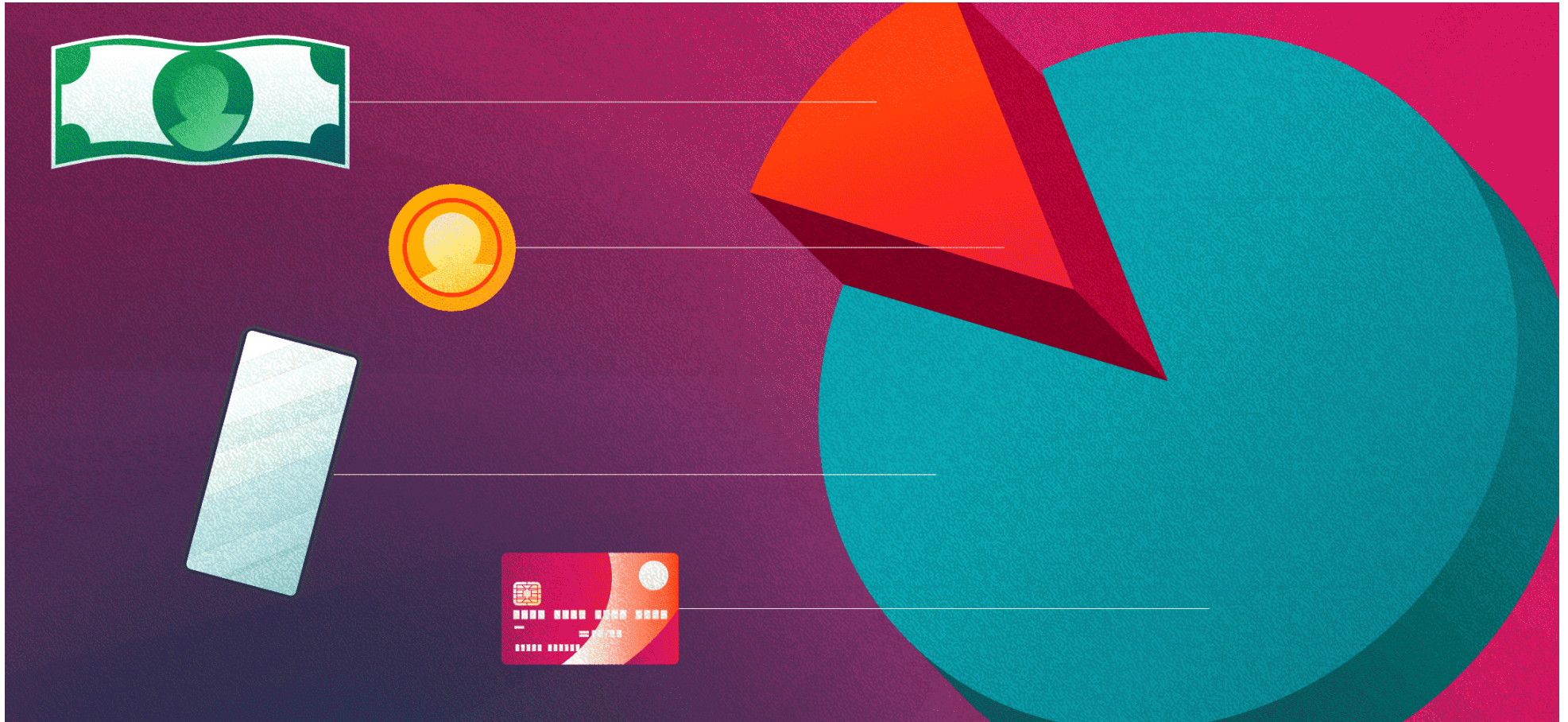




# **BITCOIN AS MONEY**



# Most Money is Already Digital



[weteachblockchain.org](http://weteachblockchain.org)



# The Functions of Money

- Store of Value
- Medium of Exchange
- Unit of Accounts



[weteachblockchain.org](http://weteachblockchain.org)



# Bitcoin Pizza Day



[weteachblockchain.org](http://weteachblockchain.org)



# Early Bitcoin Use

## Bitcoin Pizza Day

- May 22, 2010 by Laszlo Hanyecz
- 10,000 BTC for 2 pizzas
- First recorded use of bitcoin to purchase a good







# **THE TRANSACTION PROCESS**







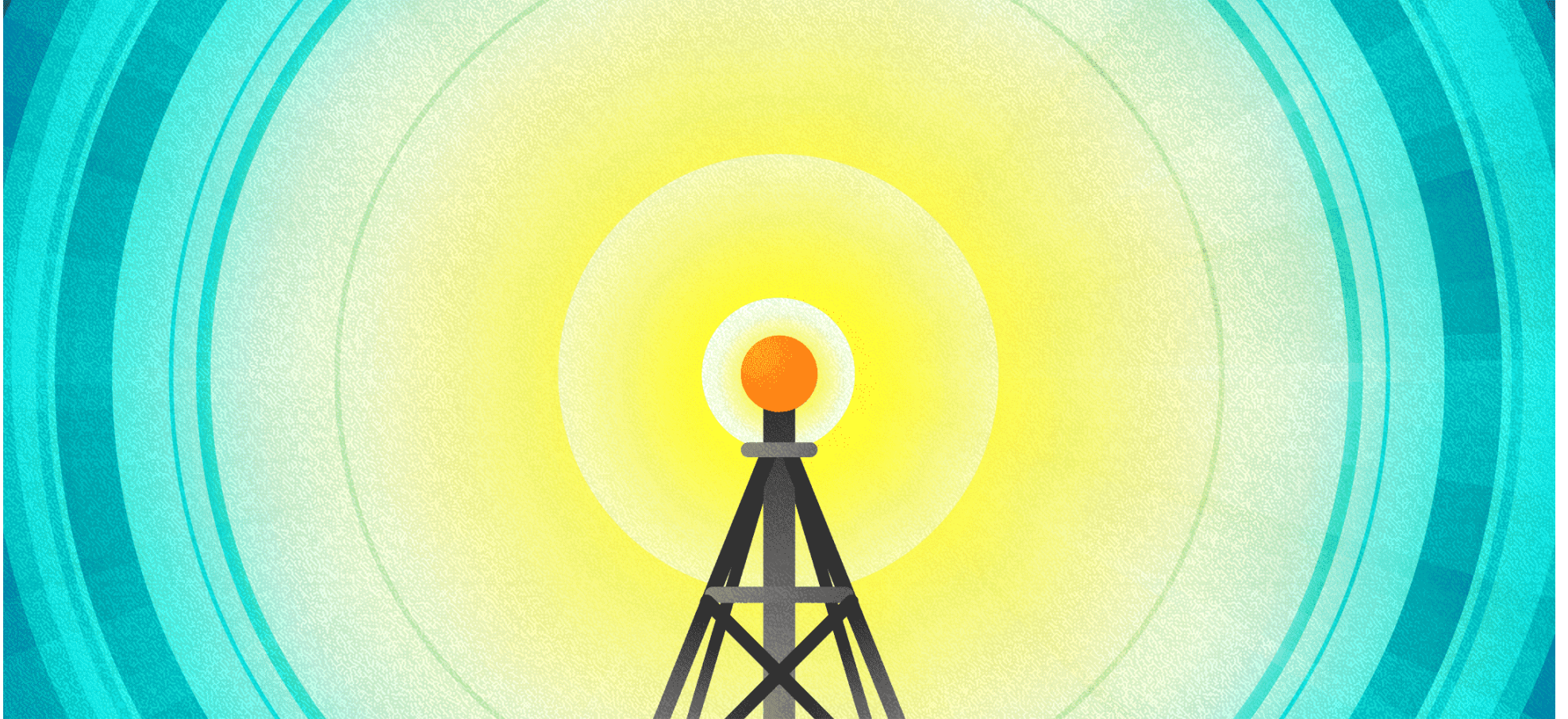
# Data Signing



[weteachblockchain.org](http://weteachblockchain.org)



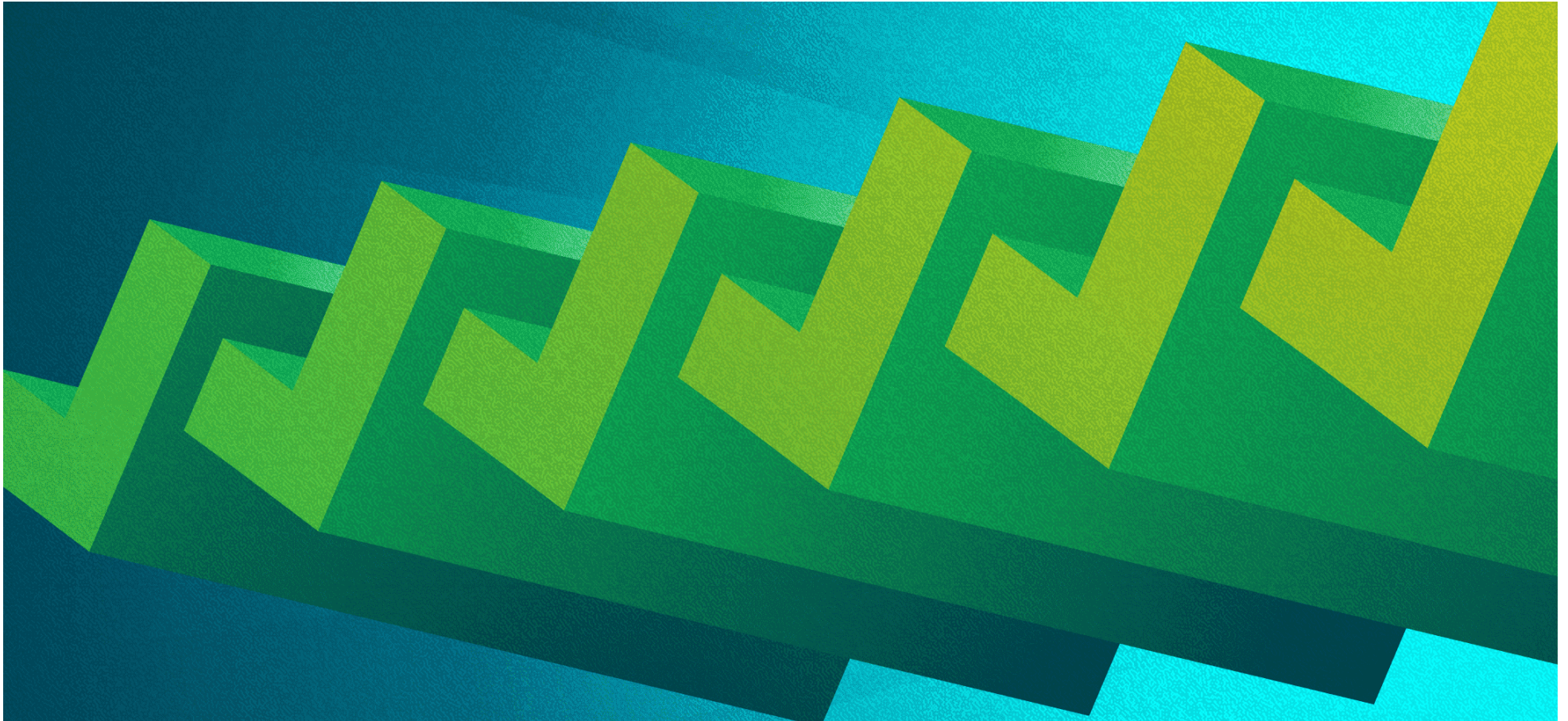
# Broadcasting the Transaction



[weteachblockchain.org](http://weteachblockchain.org)



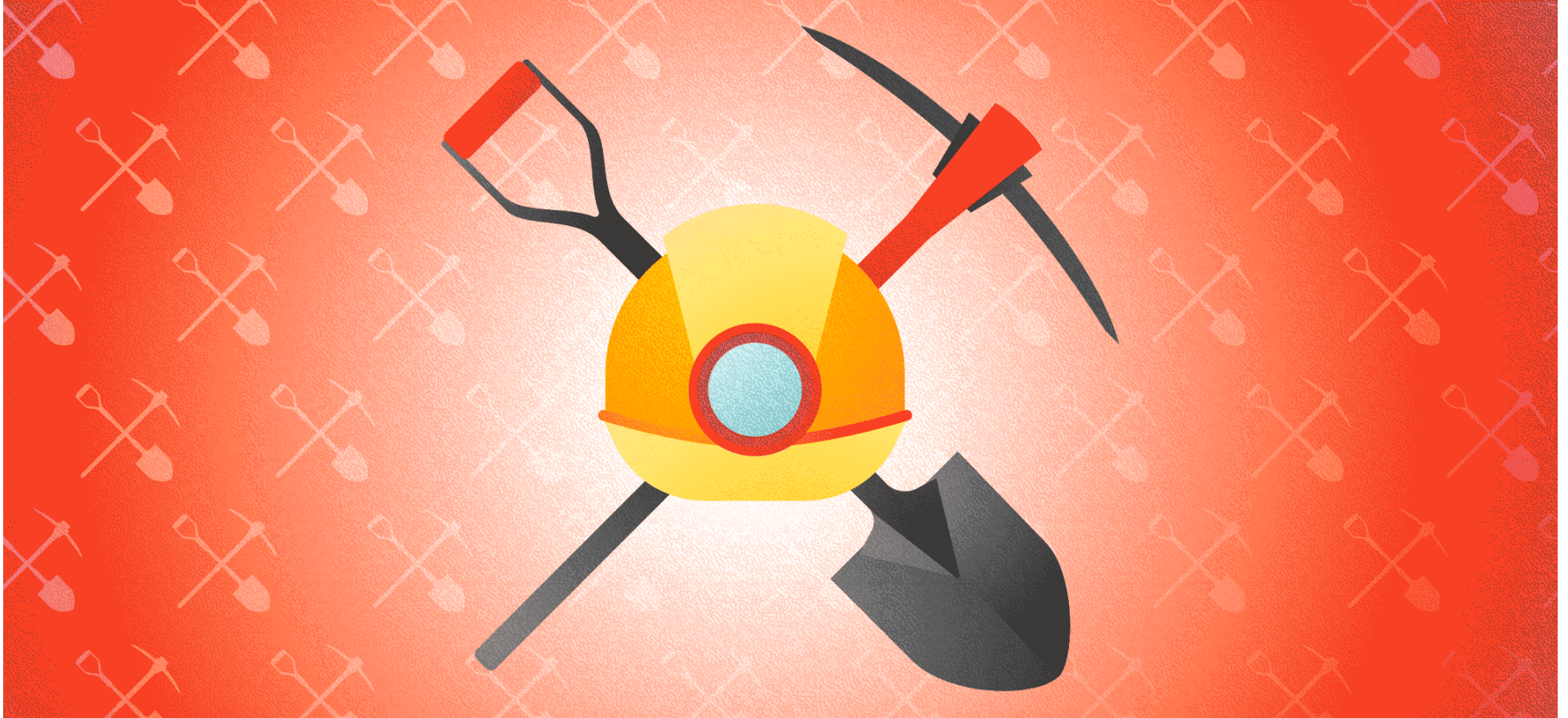
# Validation



[weteachblockchain.org](http://weteachblockchain.org)



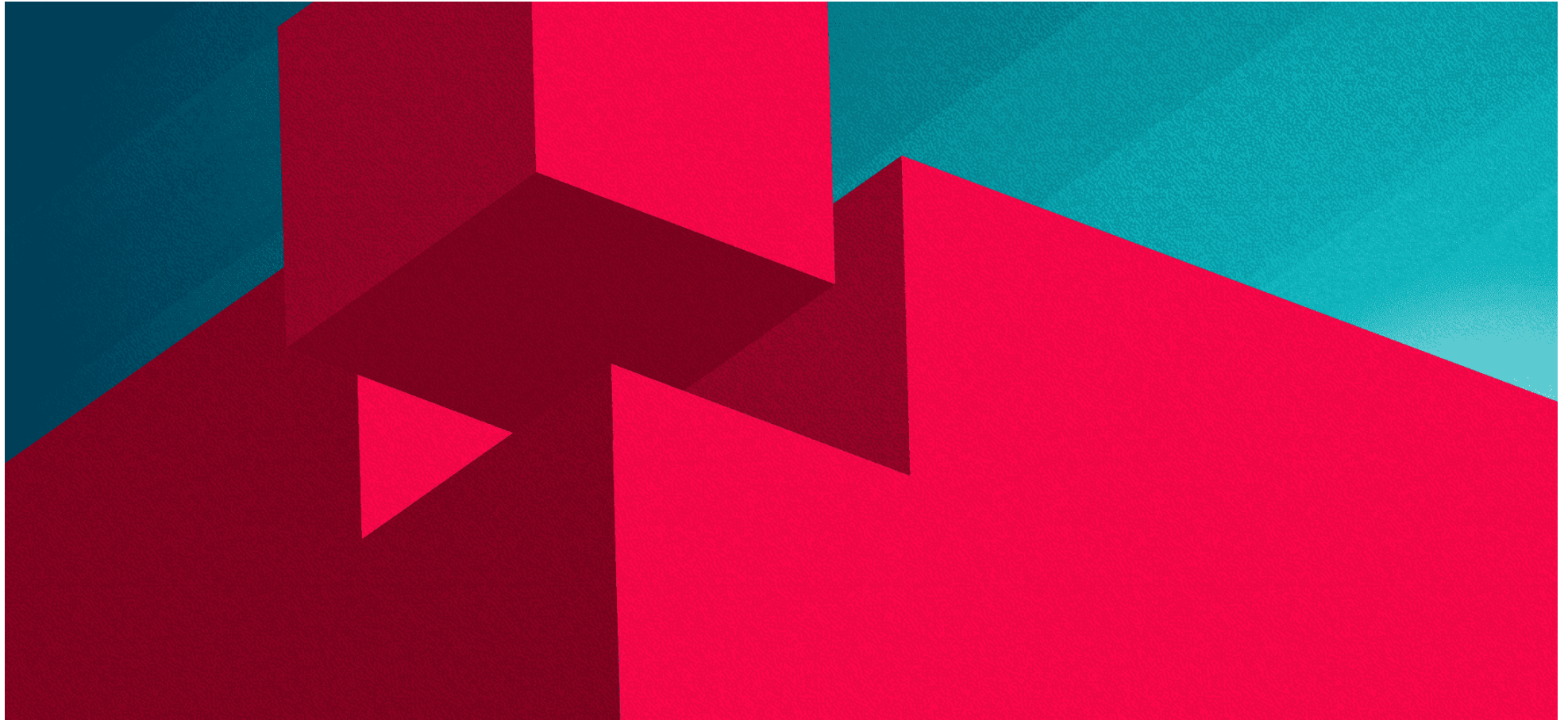
# Mempool: Before Mining



[weteachblockchain.org](http://weteachblockchain.org)



# Inclusion in a Block



[weteachblockchain.org](http://weteachblockchain.org)





**DO YOU NEED TO BE ONLINE?**

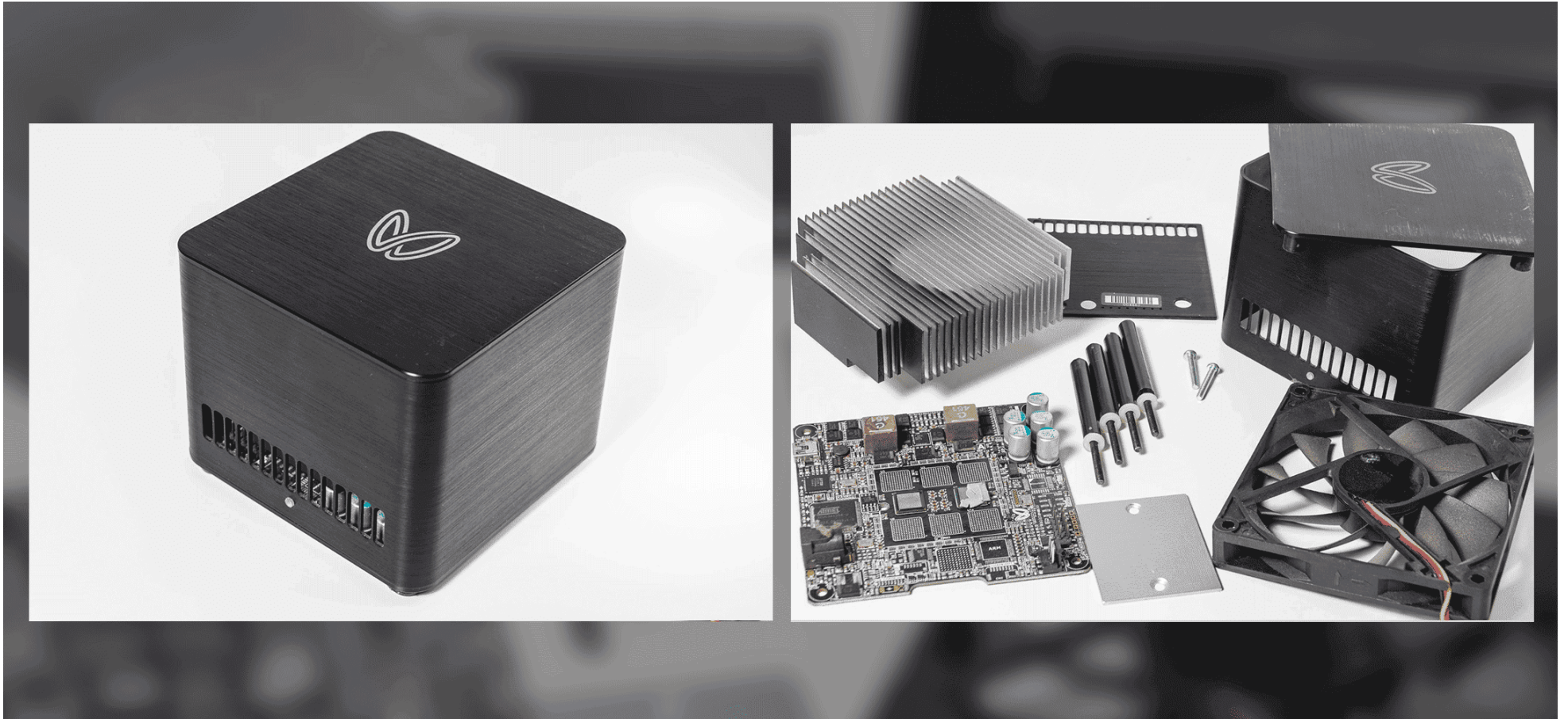




# **MINING MECHANICS**



# Inside a Mini-Miner



[weteachblockchain.org](http://weteachblockchain.org)



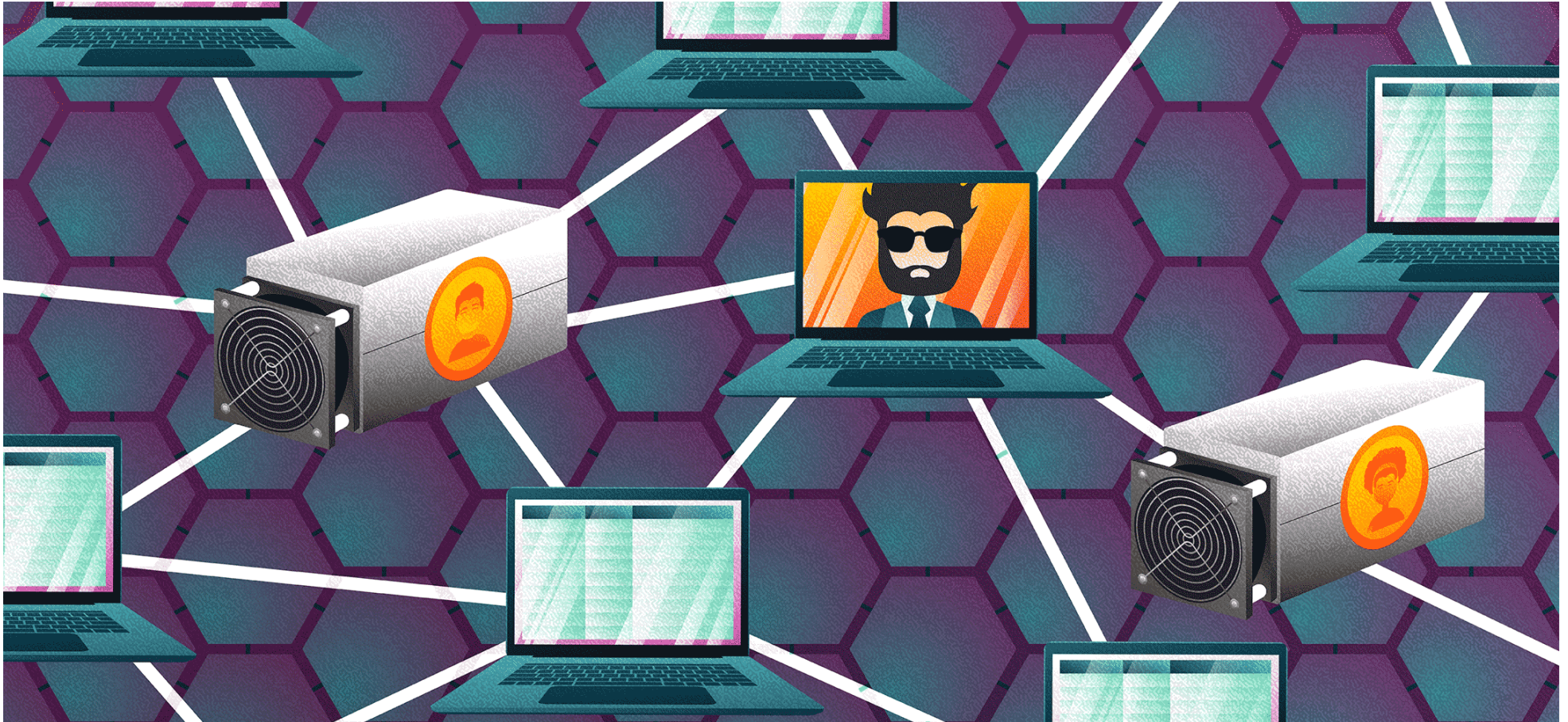
# How the Network Makes a Decision



[weteachblockchain.org](http://weteachblockchain.org)



# Which Transactions are Included?



[weteachblockchain.org](http://weteachblockchain.org)



# Hands-On Activity

## "UNDERSTANDING MINING"

*The purpose of this activity is to show how decentralized networks made up of competing miners reach network consensus.*

### DESCRIPTION

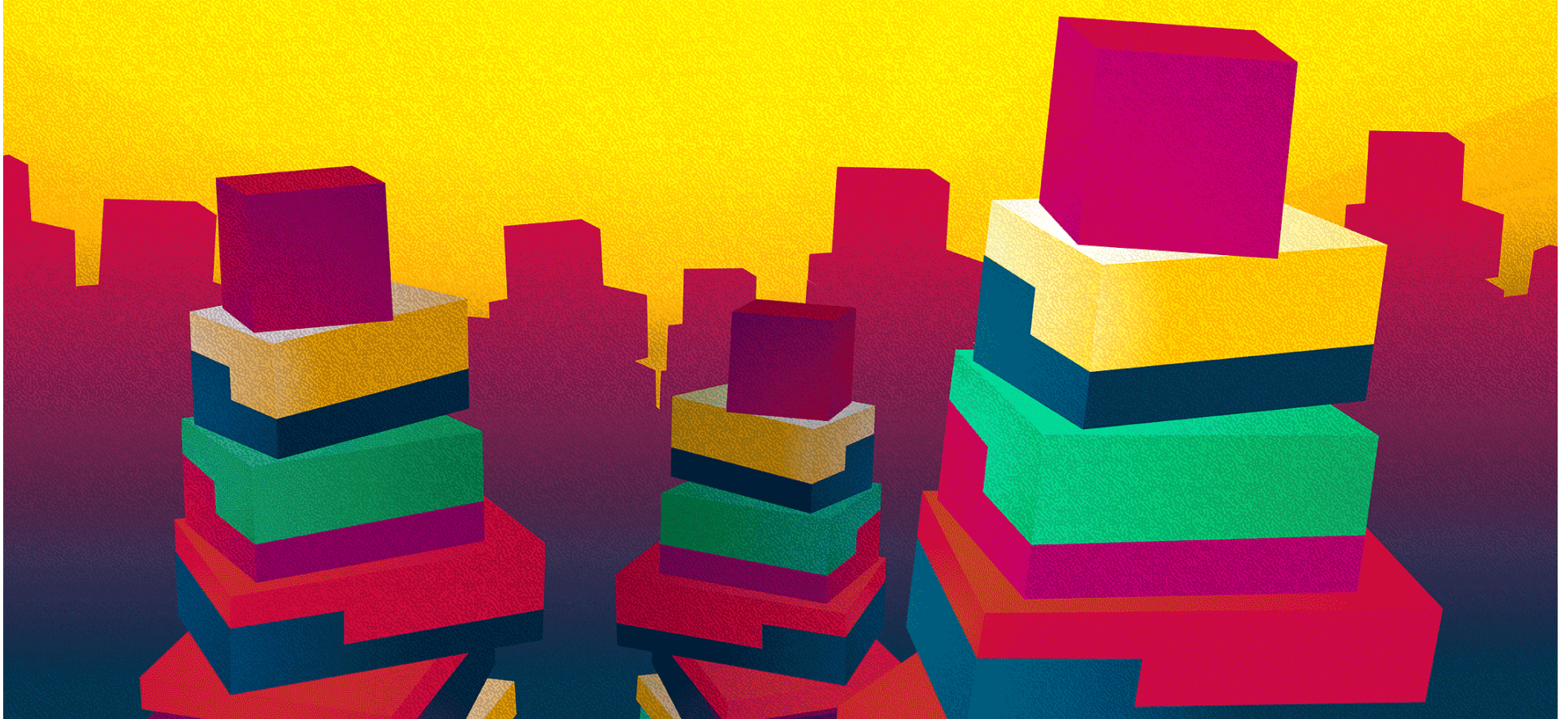
In this scenario, we are going to slow down the mining race between two miners. Each miner has a copy of Charlie's transaction for the block they are going to compile. Whichever miner that wins the race has included Charlie's transaction in the block they are creating. No matter which miner wins, Charlie's transaction gets included in the blockchain. The transactions compiled by non-winning miners are sent back to the mempool until they are added into a block by another miner.

### DISCUSSION POINTS

- Who determines which transactions get added to the block?
- What happens if my transaction does not get mined?
- What happens to Charlie's transaction if it is not immediately included in a block?



# The Block Joins the Chain



[weteachblockchain.org](http://weteachblockchain.org)



# Mining Profitability

- Probably not
- Consider cost of maintenance and management
- More cost effective to buy Bitcoin directly than converting electricity





# Transaction Fees



[weteachblockchain.org](http://weteachblockchain.org)

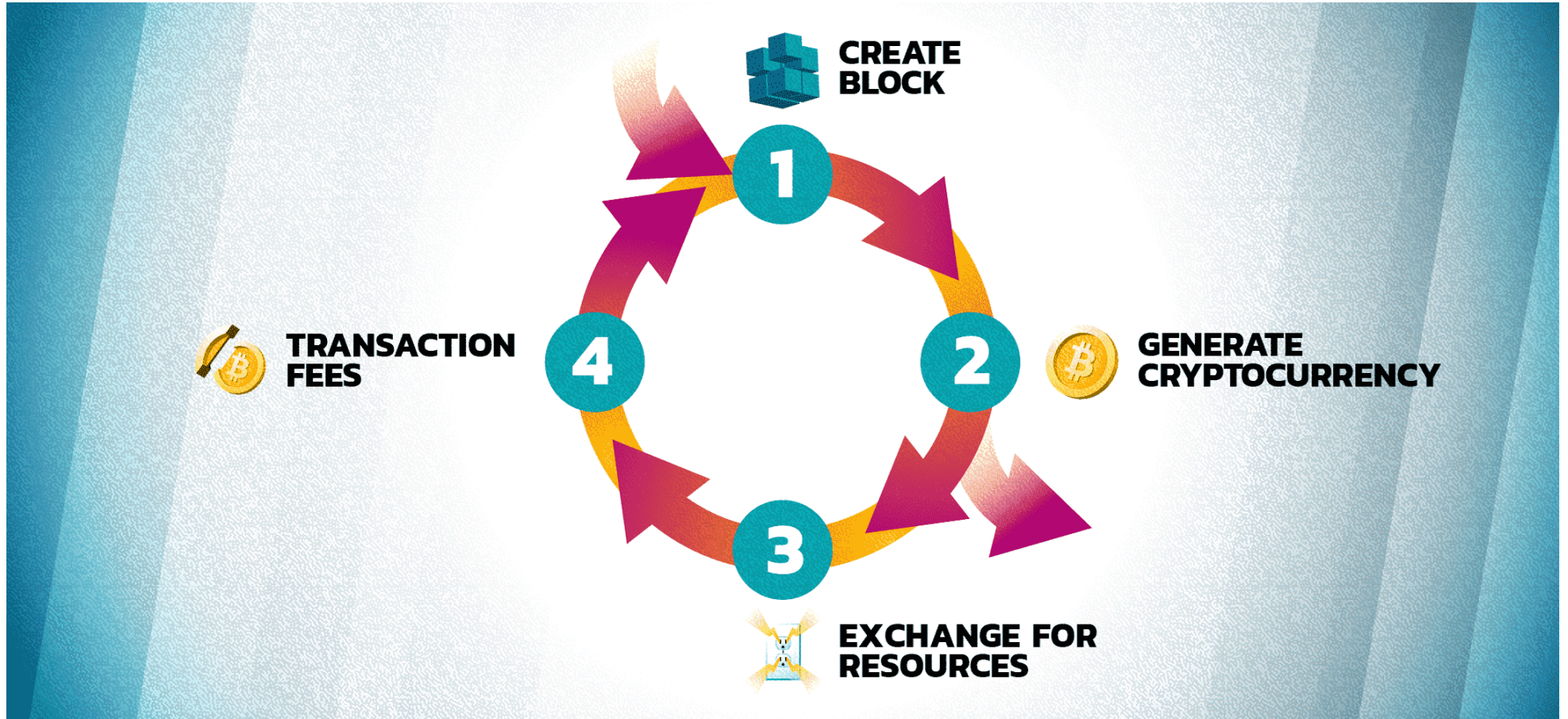




# WHERE DO FEES GO?



# Token Creation Cycle

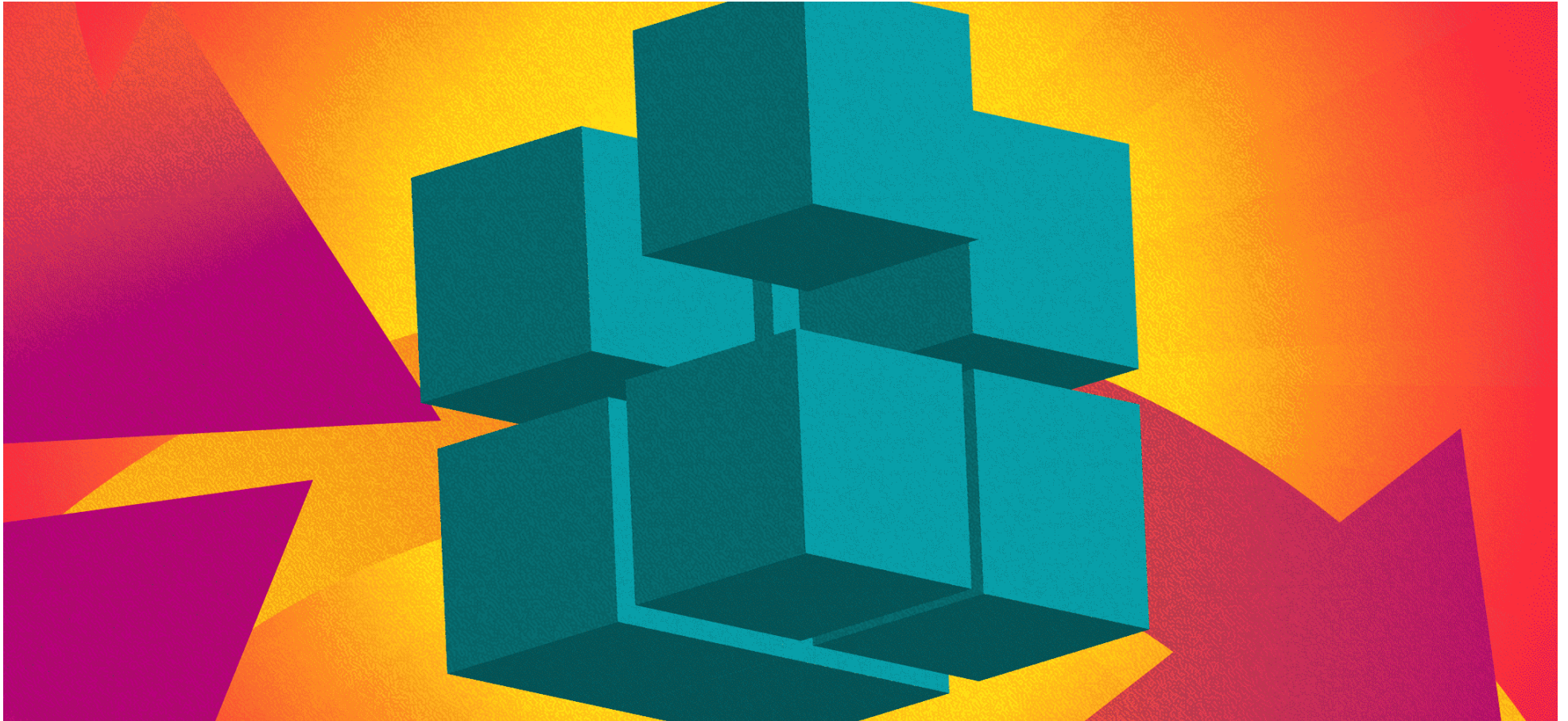


[weteachblockchain.org](http://weteachblockchain.org)

*(1) Create Block (2) Generate Cryptocurrency (3) Exchange for Resources (4) Collect Transaction Fees*



# Create Block



[weteachblockchain.org](http://weteachblockchain.org)



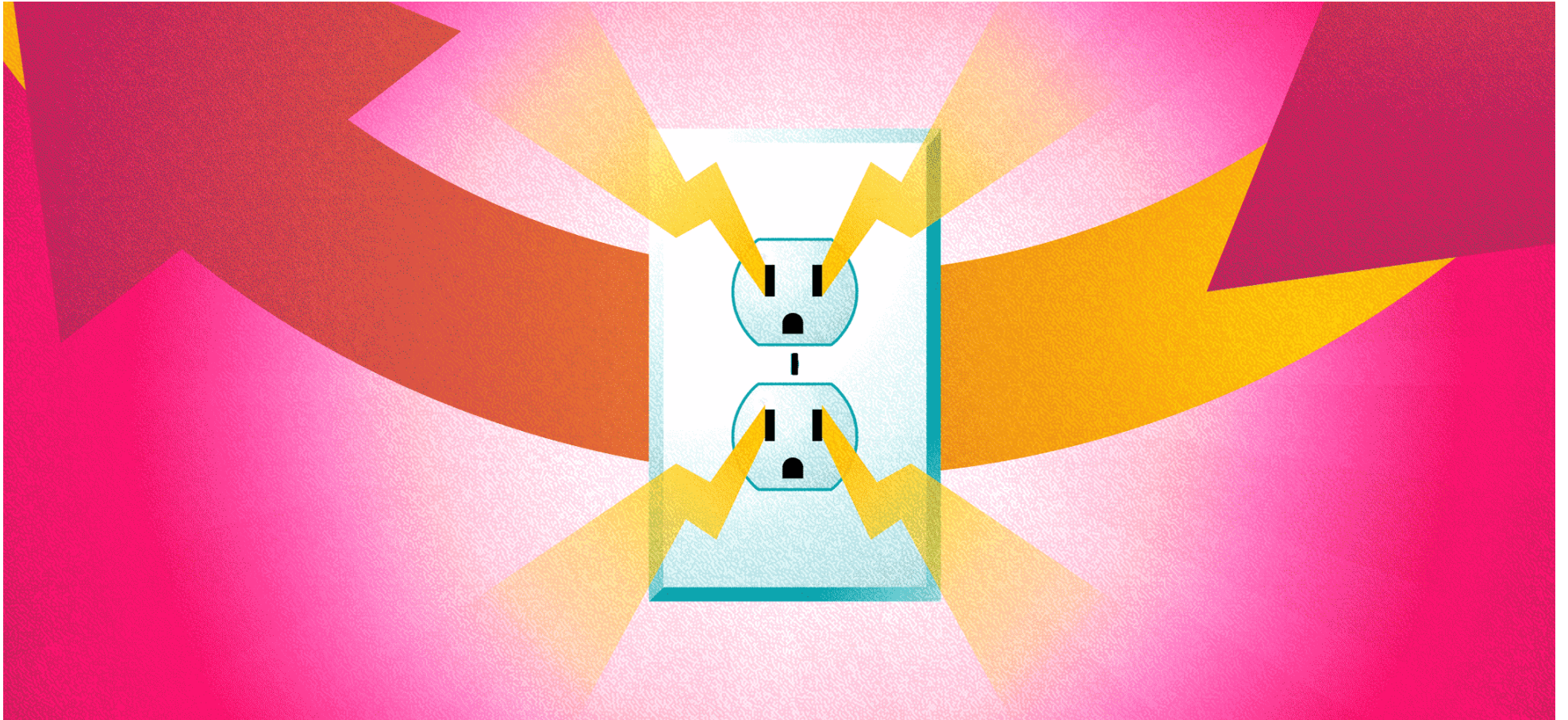
# Generate Cryptocurrency



[weteachblockchain.org](http://weteachblockchain.org)



# Exchange Tokens for Resources



[weteachblockchain.org](http://weteachblockchain.org)



# Transaction Fees Generated

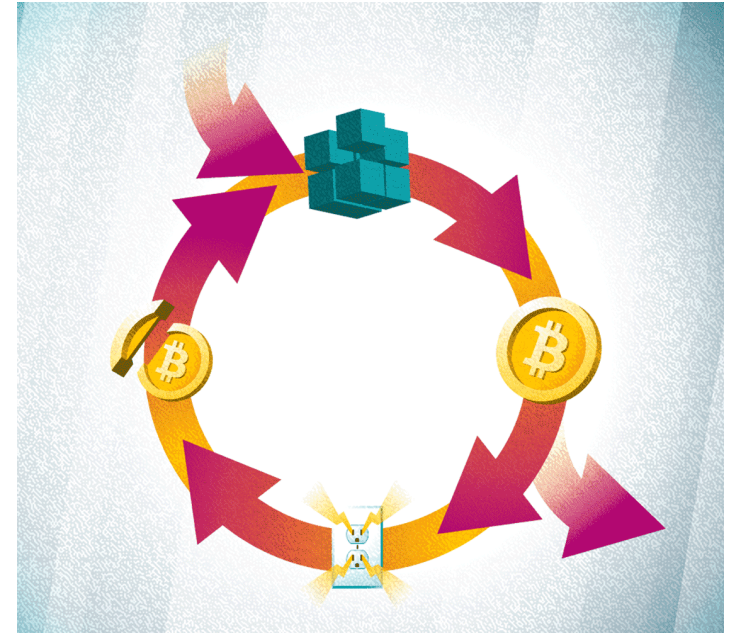


[weteachblockchain.org](http://weteachblockchain.org)



# Bitcoin Issuance Schedule

- Difficulty Adjustment
  - Maintains block production around 10 minutes
  - Adjusts every 2048 blocks (approximately 2 weeks)
- Reward Halving
  - Original rewards was 50 BTC
  - Has halved three times
  - Current reward is 6.25 BTC
  - Reward is reduced every 210,000 blocks (approximately 4 years)



[weteachblockchain.org](http://weteachblockchain.org)





# **PROGRAMMABLE MONEY**



# Blockchains Beyond Bitcoin

- Easy things to change
  - Supply
  - Confirmation time
- Hard things to change
  - Operations
  - Data structures
  - Community culture
- Other notable networks
  - Litecoin
  - Namecoin
  - Mastercoin
  - Ethereum





# More Than Money

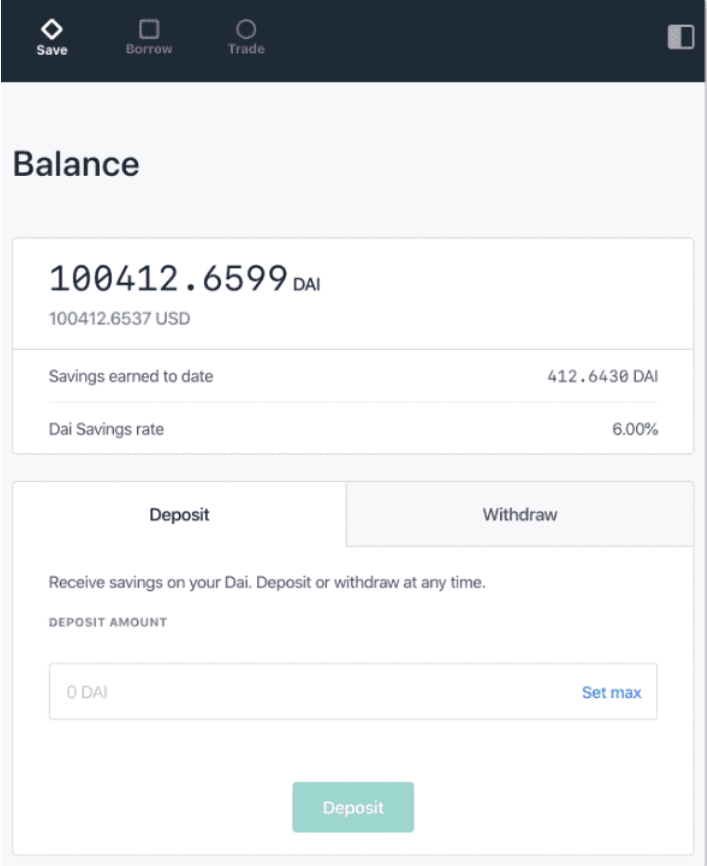


[weteachblockchain.org](http://weteachblockchain.org)



# Smart Contracts

- What is a Smart Contract?
- First Smart contracts were on Bitcoin
  - Form of crowdfunding
  - Advanced multi-signature transactions
- Decentralized Finance (DeFi)
  - Stablecoins
  - Loan & savings
  - Decentralized exchanges



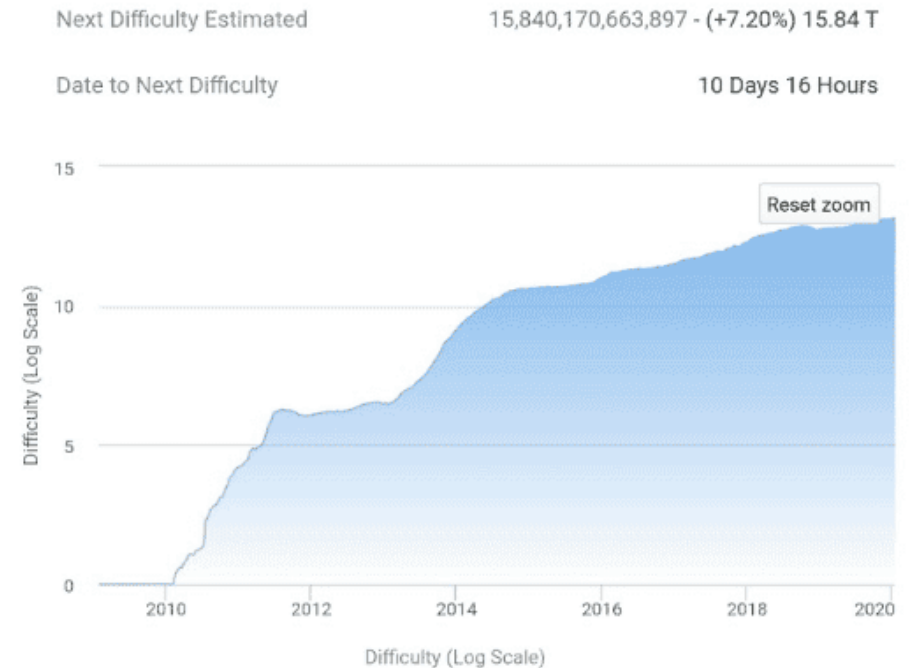
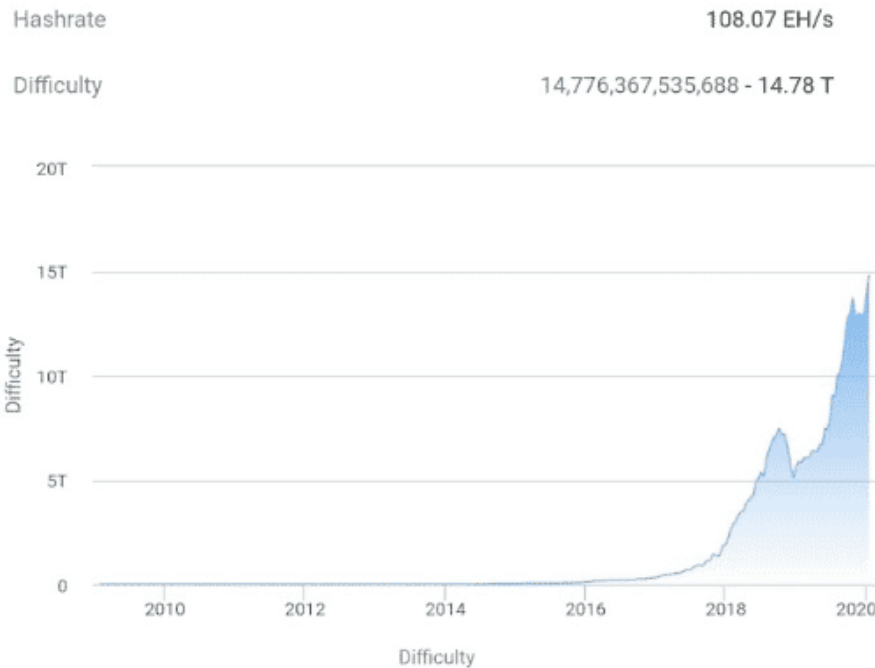
The screenshot shows the Oasis app interface for a Dai savings account. At the top, there are navigation icons for 'Save', 'Borrow', and 'Trade'. The main section is titled 'Balance' and displays a balance of 100412.6599 DAI, which is equivalent to 100412.6537 USD. Below this, it shows 'Savings earned to date' as 412.6430 DAI and a 'Dai Savings rate' of 6.00%. There are two tabs: 'Deposit' (selected) and 'Withdraw'. A message states: 'Receive savings on your Dai. Deposit or withdraw at any time.' Under the 'DEPOSIT AMOUNT' section, there is a text input field containing '0 DAI' and a 'Set max' link. A green 'Deposit' button is located at the bottom of the form.

Dai Savings Rate ([oasis.app](#)).



# Transaction Time

- What is block time?
- Bitcoin introduced 10 minute block times, a huge improvement from 3 day bank transfers
- Blockchain innovation has pushed block times down to seconds



Height	Block Time	Difficulty	Change	Bits	Average Block	Average Hashrate
612,864	2020-01-14 17:42:37	14,776,367,535,688 - 14.78 T	+ 7.08 %	0x17130c78	09 min 20 s	105.76 EH/s
610,848	2020-01-01 15:54:27	13,798,783,827,516 - 13.80 T	+ 6.57 %	0x171465f2	09 min 24 s	98.67 EH/s



# Why Blockchains Aren't Free

- Limited-use resource that costs money to transact
- This reduces spam, otherwise blockchains would become overrun like email
- Freedom of speech

## Recommended Gas Prices in Gwei

<b>8</b>   FAST < 2m \$0.027 / Transfer	<b>2</b>   STANDARD < 5m \$0.007 / Transfer	<b>1</b>   SAFE LOW < 30m \$0.003 / Transfer
--	--	---

Changes to ETH Gas Station's API

[Read on EGS NEWS](#) >

## ETH25 LEADERBOARD

Last 30 Days

RANK	NAME	ETH SPENT	AVE. GWEI	USD VALUE
1	Tether USD	1.43K	18.7	\$191K
2	ChainLink	507	18.7	\$67.5K
3	WENI	249	29.0	\$33.0K
4	dYdX	202	42.8	\$27.3K
5	Tepleton	126	24.1	\$16.7K
6	SBToken (SBC)	117	10.4	\$16.0K
7	IDEX	112	9.37	\$15.1K

Ethereum Gas Prices ([ethgasstation.info](https://ethgasstation.info))



# Credit Cards vs. Cryptocurrency

- Outdated technology
- Chargeback/finality
- “Push” versus “Pull”
  - Data storage security
- Middleman fees



[weteachblockchain.org](http://weteachblockchain.org)



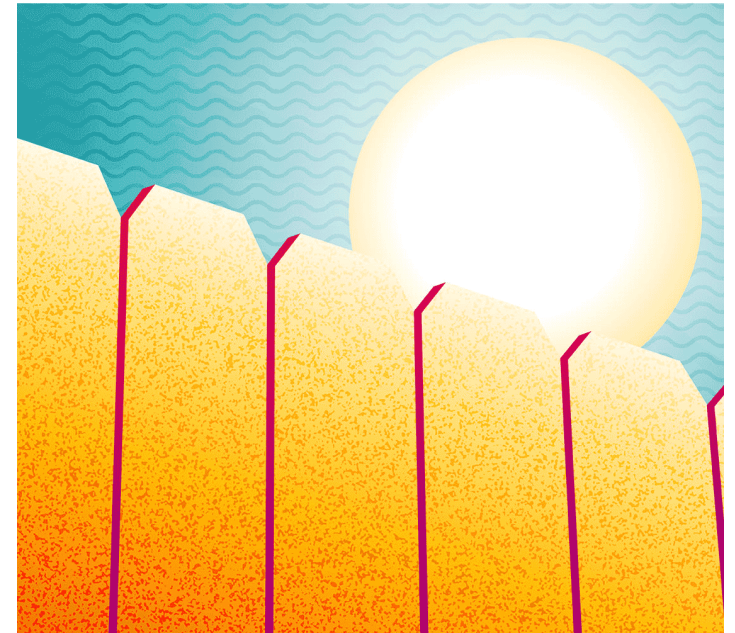


# KEEPING CRYPTO SECURE



# Transparency or Privacy?

- Details are often public (i.e. to prevent double-spending)
  - Amount
  - From
  - To
- Addresses are pseudo-anonymous
  - Possible to make lots of addresses cheaply
  - No gatekeeper or tangible cost to do so
- Privacy Techniques
  - Projects exploring different methods of obfuscation





# Address Reuse and Privacy



[weteachblockchain.org](http://weteachblockchain.org)





# **WHAT ARE CRYPTOCURRENCY WALLETS?**



# Public and Private Keys



[weteachblockchain.org](http://weteachblockchain.org)



# Seed Phrases

1

WITCH

7

DESPAIR

2

COLLAPSE

8

CREEK

3

PRACTICE

9

ROAD

4

FEED

10

AGAIN

5

SHAME

11

ICE

6

OPEN

12

LEAST



# Custodial vs. Non-custodial Wallets



***“NOT YOUR KEYS, NOT YOUR CRYPTO”***

Andreas M. Antonopoulos

Credit: [Youtube.com](https://www.youtube.com)



# Restoring Your Wallet

Enter your seed phrase:

witch collapse practice feed shame open de





# CRYPTOCURRENCY WALLETS



# Types of Cryptocurrency Wallets

- Different wallets support different tokens
- Different wallets function differently
  - Hot Wallet (“spending”)
  - Cold Wallet (“savings”)





# Hardware Wallets



[weteachblockchain.org](http://weteachblockchain.org)



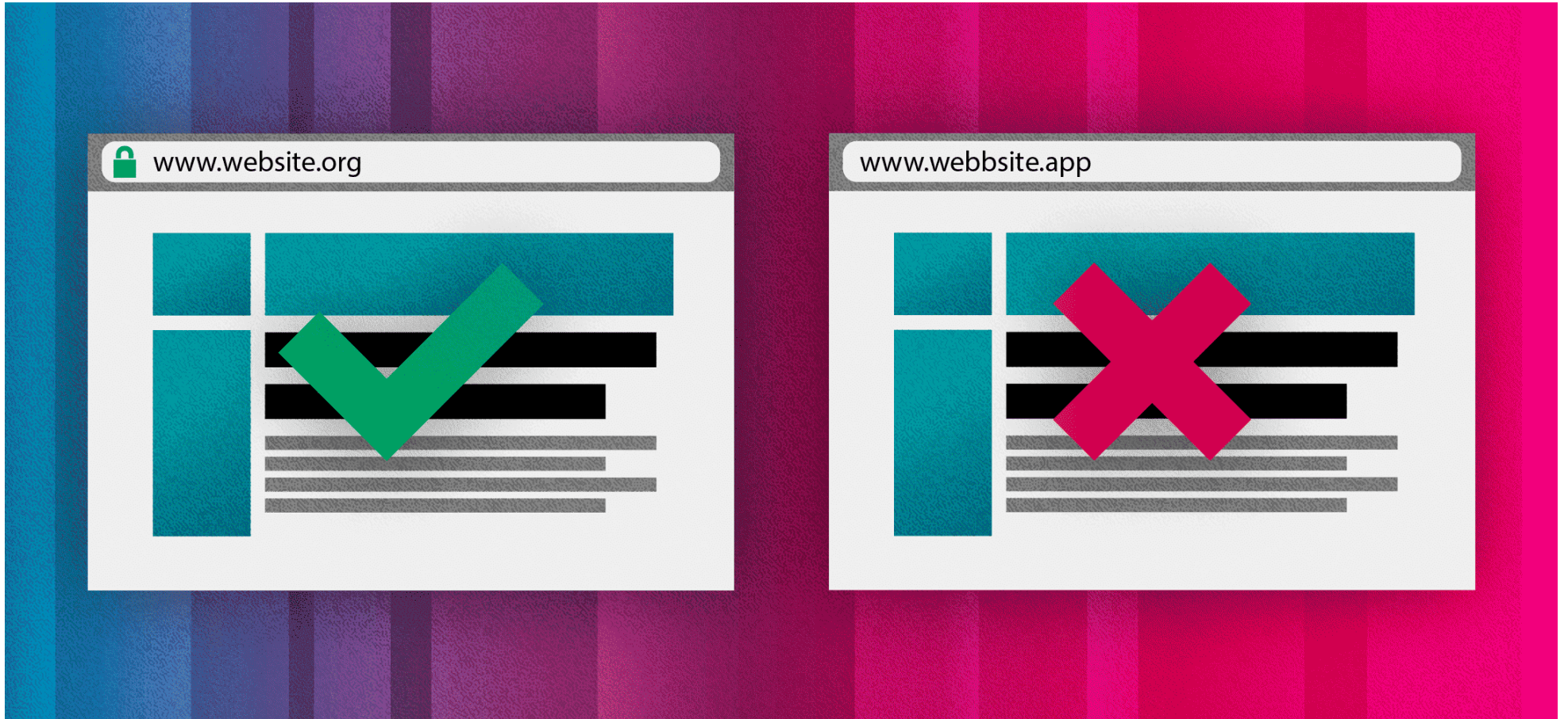
# Software Wallets



[weteachblockchain.org](http://weteachblockchain.org)



# Web Wallets





# Paper Wallets







# **INSPECTING A TRANSACTION**



# What Happened to My Transaction?

- Stuck in mempool?
- Insufficient fee or gas?
- Check for your transaction ID on a public block explorer



Screenshot from TradeBlock



# How Blockchains May Differ

## **Block Time**

The amount of time it takes for miners to solve that math problem and compile valid transactions into a block. Different blockchains have different block times.

## **Privacy**

Certain cryptocurrencies limit the amount of data that is publicly visible in order to ensure the maximum possible level of privacy.

## **Community**

Each community is different, and are motivated by different values.

## **Algorithms**

Blockchains require lots of computation, so a variety of consensus algorithms, state tracking, and hashing algorithms may be used.





# **HOW BLOCKCHAINS ARE SECURED**



# Incentive Engineering

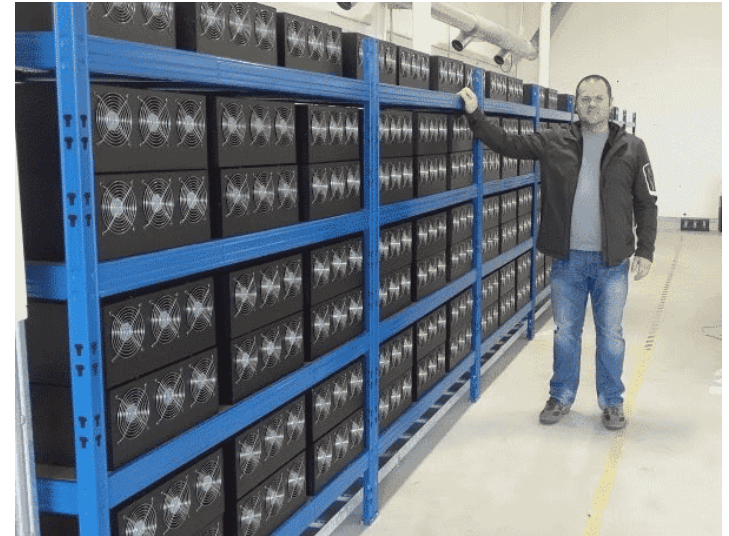


[weteachblockchain.org](http://weteachblockchain.org)



# 51% Attack: Controlling A Network

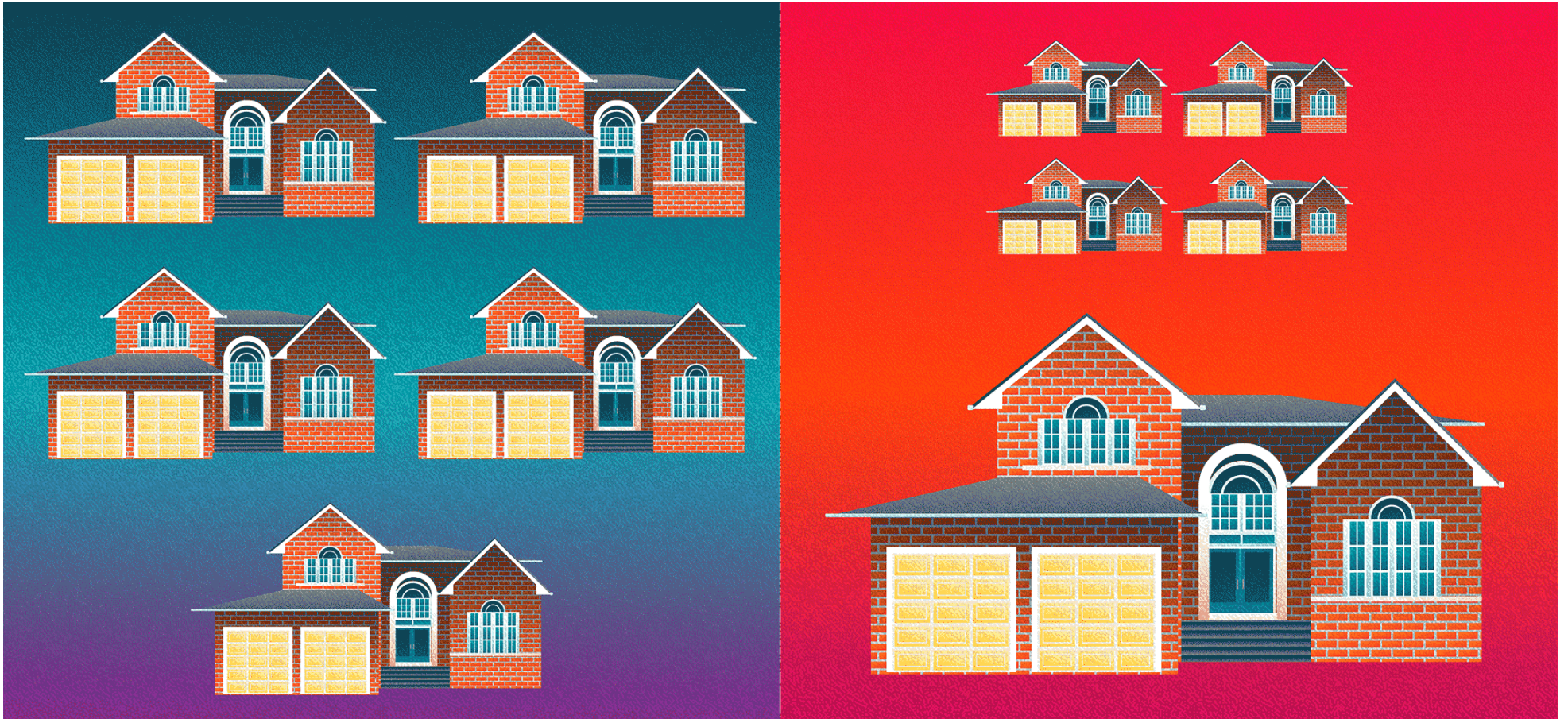
- Possible to buy computing power (AWS, Azure, etc.)
- Controlling majority hash power could allow re-writing of historical chain data
- Important to ensure diversity of network participants while maintaining incentive alignment



*Mining Facility ([bitcoinwiki.org](https://en.bitcoinwiki.org/wiki/Mining_facility))*



# Decentralized Security



[weteachblockchain.org](http://weteachblockchain.org)





# WHAT YOU CAN DO WITH CRYPTOCURRENCY

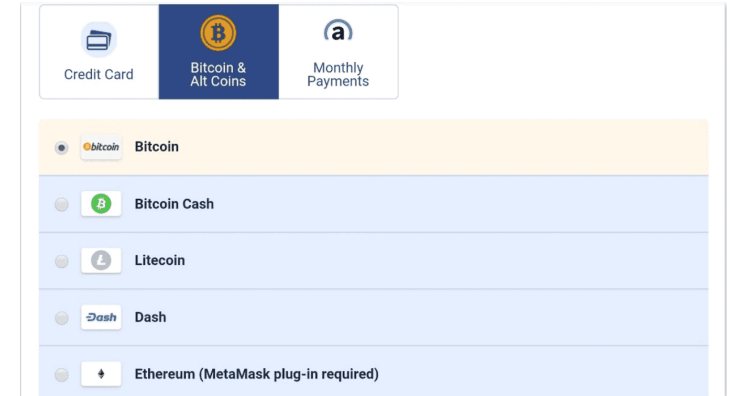






# Companies Accepting Crypto

- Wikipedia (Donations)
- Overstock (General merchandise)
- Expedia (Hotel bookings)
- Microsoft (Microsoft Store credit)
- Virgin Galactic (Space flight)
- CheapAir (Airline bookings)
- NewEgg (Technology equipment)



*Buy Flights with Cryptocurrency ([cheapair.com](https://cheapair.com))*



# Money Without Borders



[weteachblockchain.org](http://weteachblockchain.org)



# Trading



[weteachblockchain.org](http://weteachblockchain.org)



# HODLing



[weteachblockchain.org](http://weteachblockchain.org)





# **FUTURE VISION AND BLOCKCHAIN USE CASES**



# Blockchain and Business

Smart contracts have the possibility to revolutionize how business is done over the internet

May lead to innovation in a variety of industries:

- Supply Chain
- Education
- Accounting
- Governments
- Non-profits



[weteachblockchain.org](http://weteachblockchain.org)



# Provenance/Supply Tracking



[weteachblockchain.org](http://weteachblockchain.org)



# Certifications and Credentials



[weteachblockchain.org](http://weteachblockchain.org)

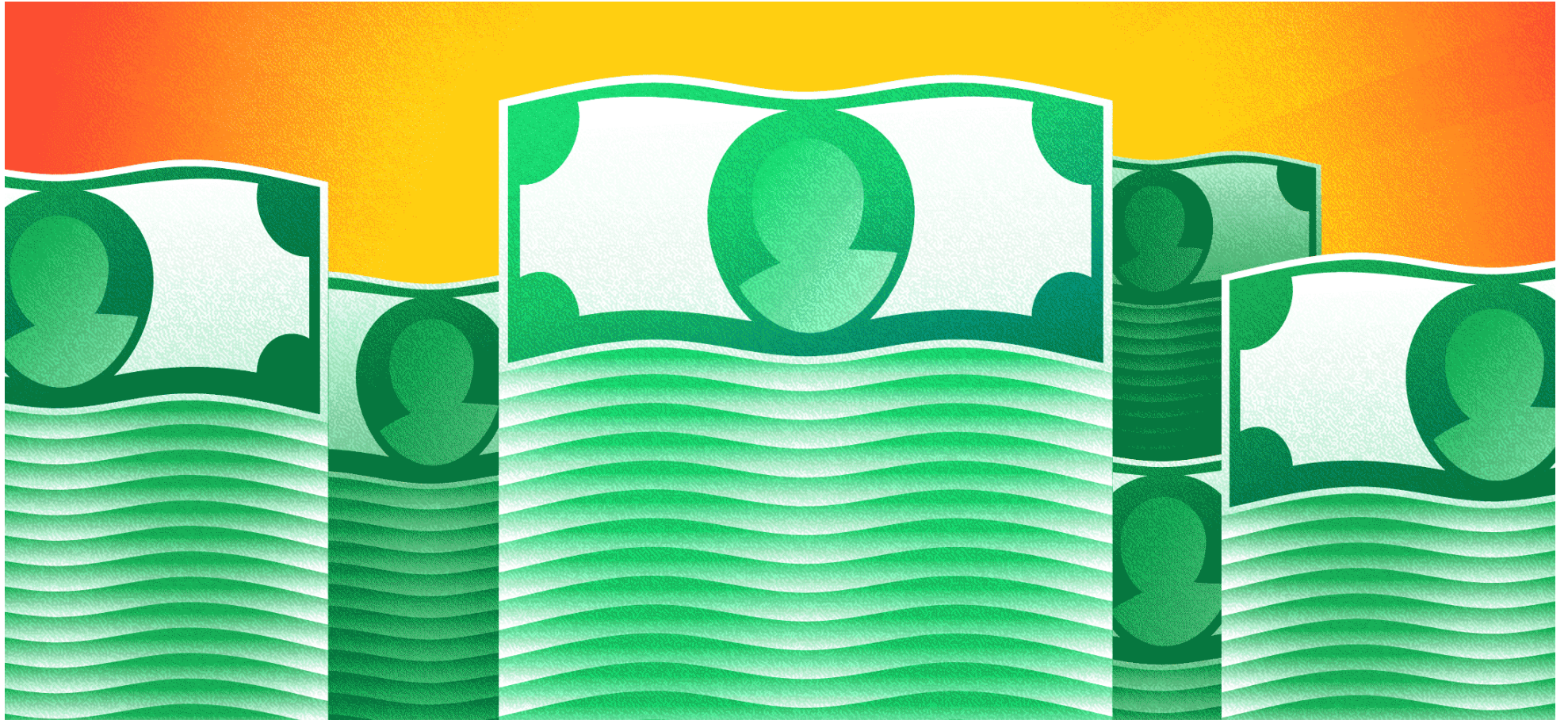


# Accounting





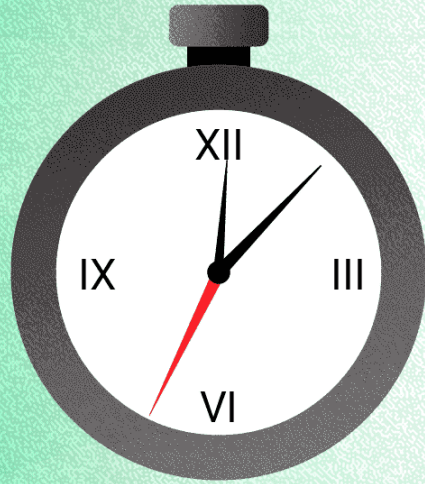
# Banking



[weteachblockchain.org](http://weteachblockchain.org)



# Non-profit



[weteachblockchain.org](http://weteachblockchain.org)



# Self-Sovereign Identity



[weteachblockchain.org](http://weteachblockchain.org)





**BLOCKCHAINS ARE NOT PERFECT**



# Privacy

- Blockchain require transparency
  - Some information must be shared
  - But what?
- Different types of Privacy
  - Data itself
  - Amounts
  - Metadata
- Potential Solutions
  - Coin Join
  - Zero-Knowledge Proofs
  - Homomorphic Encryption

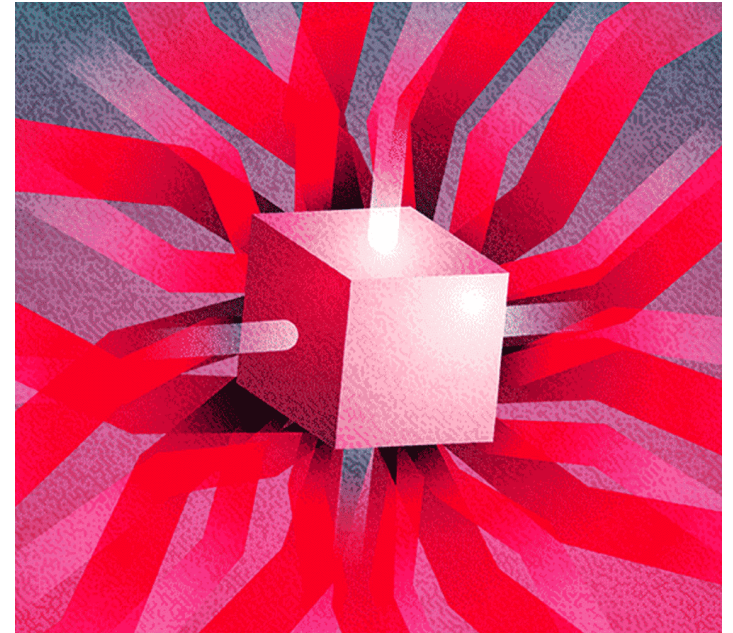


[weteachblockchain.org](http://weteachblockchain.org)



# Scaling for Global Usage

- Expensive due to inefficiency
- Network bandwidth & disk space are finite resources
- Current technology cannot support global population of 8 billion
- Transaction backlogs and high fees would result
- Possible solutions
  - Second Layer
  - Sharding

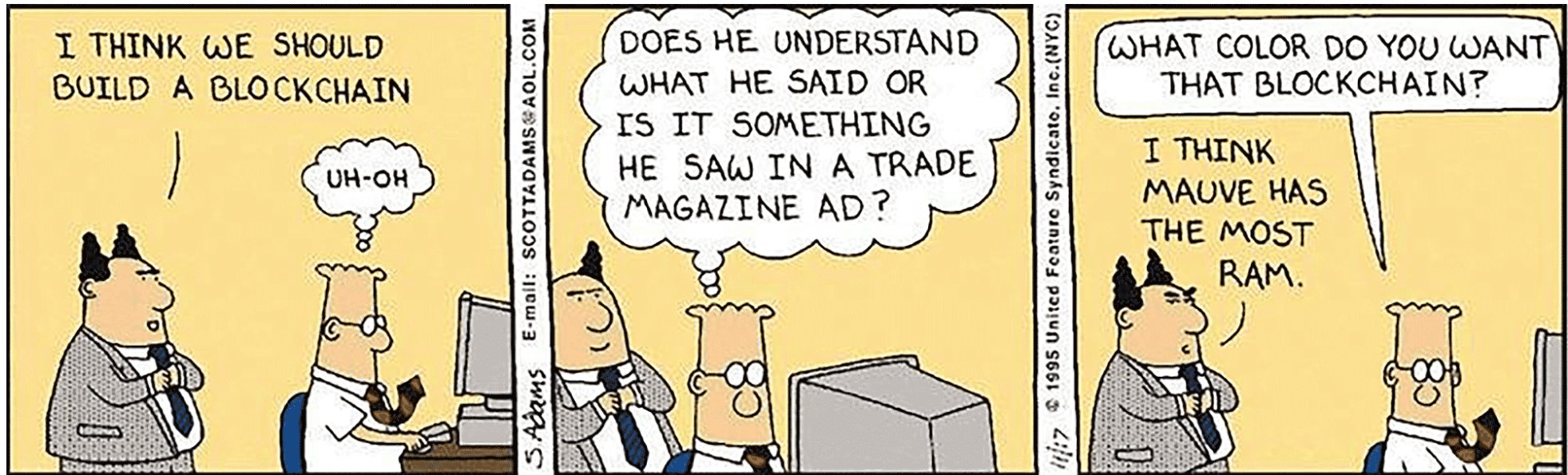


[weteachblockchain.org](http://weteachblockchain.org)



# Unanswered Questions

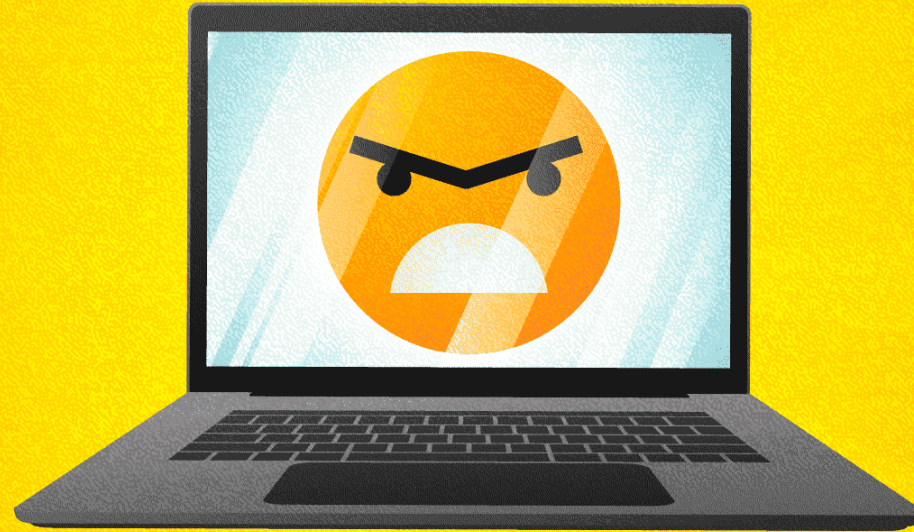
- Governance
  - What do you do when things go wrong?
- Incrementalism
  - Are you too dependent on the technology?
- Appropriateness
  - Is this data useful/needed forever?



Blockchain Comic ([dilbert.com](http://dilbert.com))



# Not User-Friendly Enough



[weteachblockchain.org](http://weteachblockchain.org)

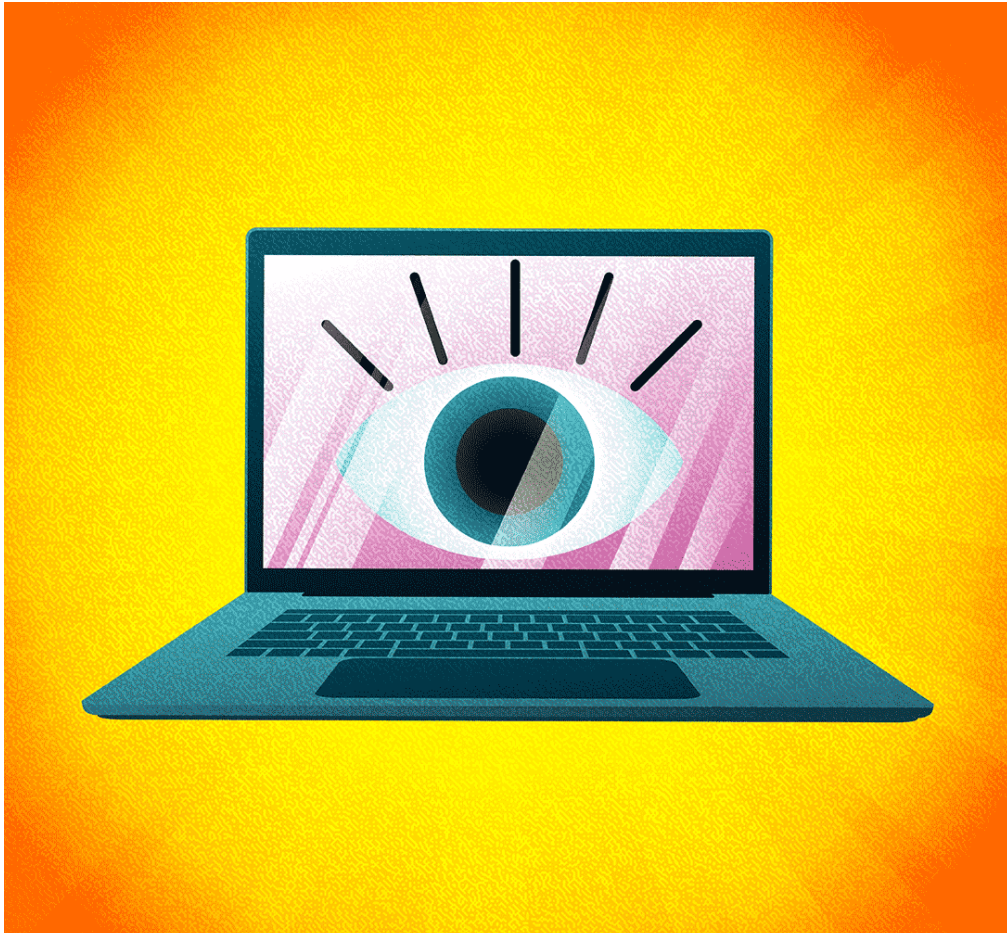




**BUT STILL WORTH USING!**



# Modern Challenges

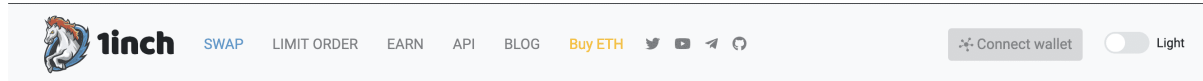


[weteachblockchain.org](http://weteachblockchain.org)



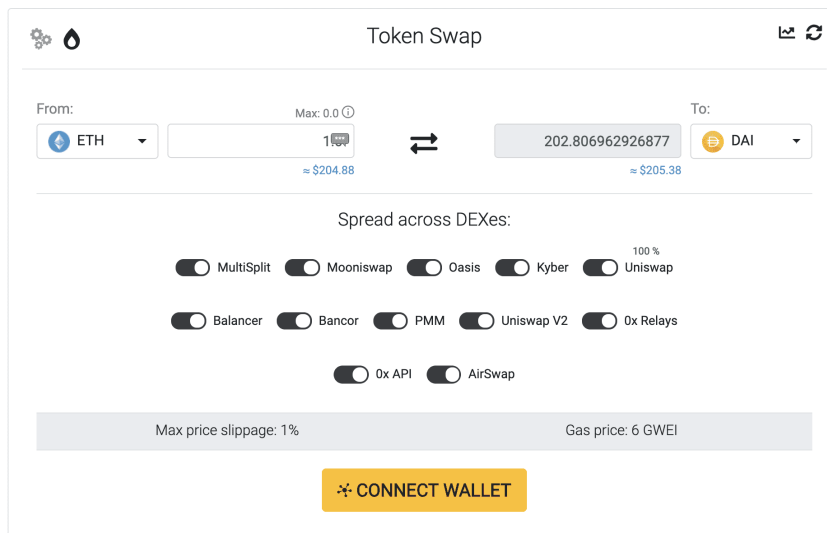
# Technological Tools

- Resiliency against fragile internet infrastructure
- Defend our freedoms to transact value directly
- Cryptography as digital armor



DEX Aggregator with the best prices on the market.

Achieving best rates by splitting orders among multiple DEXes in one single transaction.



The 'Token Swap' interface shows a swap from ETH to DAI. The 'From' field is set to ETH with a value of 1 ETH (approx. \$204.88) and a 'Max: 0.0' limit. The 'To' field is set to DAI with a value of 202.806962926877 (approx. \$205.38). Below the swap fields, there are toggle switches for various DEXes: MultiSplit, Mooniswap, Oasis, Kyber, Uniswap (100%), Balancer, Bancor, PMM, Uniswap V2, 0x Relays, 0x API, and AirSwap. At the bottom, it displays 'Max price slippage: 1%' and 'Gas price: 6 GWEI'. A prominent yellow 'CONNECT WALLET' button is located at the bottom center.



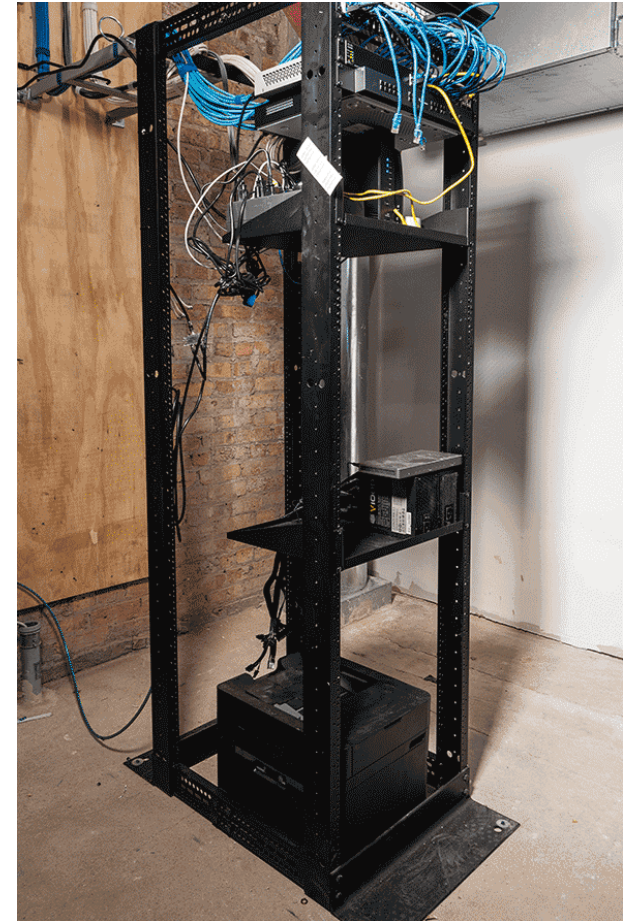
# Web3

## Bringing Decentralized Technology to our internet

- Removing intermediaries means you can transact more directly
- Gives creators more options on how to generate revenue

## Microtransactions

- Decentralizing the web could lead to better capacity allocation
- The introduction of digital uniqueness may give rise to control over our personal data
- Re-assert the internet as a playground for everyone
  - Not only large corporations
  - Protect from state attacks



[weteachblockchain.org](http://weteachblockchain.org)



# Summary

- Storing Cryptocurrency Securely
- Hands-on Crypto Experience
- Understand how a blockchain transaction works
- Define cryptocurrency and how it's different than traditional money
- How blockchain may impact the world

---

## Course Goals

- Learn how to store cryptocurrency securely
- Execute your own cryptocurrency transaction
- Know where to look when something goes wrong
- Explain how cryptocurrency is different than cash
- Understand how blockchain technology may impact YOU!





# Q&A



# How to Join Us

[Sign up for our Newsletter!](#)

Follow us on social media!

- Twitter: [@bchaininstitute](#)
- Facebook: [theblockchaininstitute](#)
- Instagram: [theblockchaininstitute](#)

Apply to become a [Blockchain Ambassador!](#)



[weteachblockchain.org](http://weteachblockchain.org)